Attachment to Complaint

Section III Statement of Claim

1. Defendant Skype Communications S.à.r.l. is a telecommunications company whose application allows its users to message and chat with each other for free and allows its users to call non-users on a phone number for a fee. While Skype operates a distinct website and an app that bears its name and provides and collects payments for the telecommunications services to its customers, Defendant Microsoft Corporation is in charge of security, maintenance, and customer relations of Skype users' accounts. In this the two defendants operate a common enterprise of telecommunications business.

2. Microsoft offers numerous other services and operates several websites, including bing.com, where customers may sign up for Microsoft accounts, some of which are fee-based and some of which are nominally free to users and supported instead by other sources of revenue, most notably advertising, which grows through Microsoft's collection, aggregation, combination and/or analysis of users' information. Microsoft is in charge of security, maintenance, and customer relations of Microsoft users' accounts.On or before December 11, 2018, Plaintiff signed up for a Skype account through Skype's website or app and in doing so accepted the latter's terms of service titled "Microsoft Service Agreement". Plaintiff likely accessed Skype's website or app through a public or shared Internet Protocol ("IP") address because Microsoft revealed in 2021 that they logged Plaintiff's IP address at the time and found it identical to the address of at least 258 other accounts, most of which Microsoft considered to be engaging in suspicious activities and denied service to.

3. Later that day, Plaintiff made a $10 purchase to enable him to use his Skype service to make calls to non-Skype phone numbers when traveling abroad. Since Skype's creation, many messaging apps have overtaken it in popularity, but Skype retains its market dominance as an app that allows a user to call a non-user on the non-user's phone, and Plaintiff was and is unaware of alternative products to Skype when traveling internationally. Further, the app came pre-installed in Plaintiff's computer that operates on Windows, a product of Microsoft.

4. It is now revealed that at the time of his payment for the Skype service on December 11, 2018, Microsoft's automated systems deemed Plaintiff's IP address as a low "Reputation Score" IP such that the automated systems would prevent him from using the services that he was paying for. In other words, Plaintiff was already guaranteed to receive no consideration in return for his money under the terms of contract.

5. On January 20, 2019, when Plaintiff tried to log into his Skype account through Skype's app when staying at a hotel abroad and likely through a public IP that Defendants again logged, he was told that something went wrong and that he needed to sign in through a browser and through a Microsoft website. On that website, upon putting in his username and password, Plaintiff was told his account was suspended because spam was sent from his account or some other account activities were in violation of the service agreement. The webpage said that Plaintiff must share his mobile number and Microsoft must send him a text message before he could resume using Skype service. Despite his privacy and security concerns of sharing his phone number with the defendants and of using his US phone in a foreign country, Plaintiff reluctantly did as he was asked in order to make an urgent international call and was then able to sign in both via Microsoft's website and to Skype app.

6. Following the incident and on or around January 24, 2019, Plaintiff wrote to Microsoft to request details on the allegations of sending spam and/or other violations of the service agreement that had resulted in the loss of his use of Skype service. He was given no clear answer except that Microsoft barred his access to the Skype account "to make sure it was safe". Further, a Microsoft webpage that Plaintiff was directed to intimated the blocked access would suggest that Plaintiff's account suffered from "malware, phishing attacks, or other harmful activities".

7. These vague warnings of account safety gravely alarmed Plaintiff and compelled him to scrutinize all his emails in the email account used for his Skype account: he was going through thousands of my emails to see whether there were any messages in the Sent folder that he didn't create, any incoming messages that suggest that someone received emails that he didn't send. Further, he had to secure many third-party app or website log-ins that used this particular email. And because Microsoft was persistently and stubbornly secretive and evasive

through 2019 and 2020 about the exact nature and timing of the suspected "malware, phishing attacks, or other harmful activities", Plaintiff had to constantly monitor all third party apps and accounts that were associated with his Skype account's log-in to catch on any unusual activities as well as his credit history and financial accounts' activities.

8. Plaintiff had also created a Microsoft account on one of Microsoft's website, likely bing.com, at some point before June 18, 2019, and was trying to sign into that account that day to use credit in the account to redeem a promotional offer of Microsoft products. Upon putting in his username and password, Plaintiff again landed on a page that said this account was suspended because spam was sent from this account or some other account activities were found to be in violation of Microsoft's service agreement. The page, too, said that Plaintiff must share his mobile number before he could resume using Microsoft services.

9. This time Plaintiff left that page and searched for Microsoft's technical support and was connected with an agent, Abigaile A. The agent wrote to Plaintiff that it was most likely that "someone has access on your account or trying to access your account". She then unlocked Plaintiff's account by verifying a code she sent to Plaintiff's email address associated with the account, an option that Microsoft hid from its webpages. Yet, the agent refused to answer what nefarious actors may have gotten access to Plaintiff's account to have prompted the suspension of service.

10. Plaintiff continued to press Microsoft for more details about the breach of his Microsoft account that Microsoft's representative hinted at. But throughout 2019 and 2020 the Microsoft defendant obstinately refused to elaborate on the grave but vague warnings that it sent to Plaintiff in June 2019, citing commercial secrets about its algorithm and "the system" for its refusal to do so.

11. Only in October 2020, after Plaintiff indicated his intention to sue the two defendants, did a Microsoft paralegal, Jose Pablo Leandro, write to him that "the problem is not you sending spam" and that he reviewed Plaintiff's two accounts and confirmed that neither "has not been compromised." By then, Plaintiff had been compelled to review and monitor activities in email and other financial or credit accounts associated with his Microsoft account, much in the same manner that he had to review and monitor his many accounts associated with his Skype

account. The defendants have now stated that a customer may resume services with Microsoft and Skype accounts suspected of security compromise or suspicious or abusive use through a verification code sent to (the customer's choice of) either her mobile phone number or her email address that was used to sign up for her Microsoft of Skype account. It should be noted, however, that the defendants did not make the latter choice known to their customers. The latter choice would naturally be more palatable to the more privacy-concerned customers, but the fact is the defendants made their customers spend significant amount of time to navigate formidable customer service hurdles before they could learn about and access this choice. The notional "choice" was in fact a false one and speaks rather to the intentionality and deceptiveness of the defendants' actions.

12. Microsoft's subsequent review of Plaintiff's Skype account also concluded that Plaintiff was denied access to his paid Skype account in January 2019 for what the defendants alleged to be violations of "section 4.a.ii" of the agreement at the time. Although neither defendant came clean in 2019 or 2020 the reasons and circumstances for which they may have evoked the service agreement to terminate services, they now assert that Plaintiff's use of a public IP address was the reason of their refusal of service in 2019. (Additionally, the defendants note that their interpretation of this clause evolves month to month to include a changing list of activities that are deemed violation of the agreement, but they refuse to disclose the current list on the ground that their interpretation of the agreement is "proprietary information.")Bizarrely, the defendants also assert that Plaintiff's Skype account is considered a "free account" under the service agreement. They explain away the facial absurdity of this assertion - when Skype had taken a payment from Plaintiff for its service - by saying that "free account" is a term of art, albeit one that by their own concession is neither defined in the agreement nor even encountered by a customer at any juncture during the process of her sign-up or making payment.

13. The defendants' series of scary warnings about Plaintiff's compromised accounts and emails taken over by nefarious parties have now proven to be a ruse and a fraud to "phish" for his personal information and phone number, which Plaintiff had refused to share with the defendants when he created his Skype and Microsoft accounts. National newspapers and privacy advocates have long pointed to how big tech firms enrich themselves through not only the collection

of consumers' personal information but also *combination* of person information collected at different junctures to build more financially valuable profiles of individual consumers. Plaintiff has reasons to believe also that Microsoft has "combined" the personal information it deceptively obtained of Plaintiff in January 2019 with personal data it had collected of him prior to that point in order to drastically enhance the value of the "combined" personal data it possesses of its users and sell the data for higher prices to its advertising clients.

Section IV: Relief

14. Skype took payment on December 11, 2018 for services that it did not really intend to furnish. Its actions constituted an unfair and deceptive business practice enjoined by New York General Business Law 349. For this Plaintiff sues for $10 plus statutory and punitive damages under GBL 349.

15. When Plaintiff doggedly tried to regain access to the services he paid for, Microsoft allowed Plaintiff access only after it made Plaintiff turn over valuable personal information he would not have agreed to proffer when he made the purchase. In luring a consumer into an agreement before changing the terms that the consumer was unlikely to have agreed to in the first place, Skype and Microsoft's actions again constituted an unfair and deceptive business practice enjoined by New York General Business Law 349. For this Plaintiff sues for $10 plus statutory and punitive damages under GBL 349.

16. Skype's actions in advertising and taking or processing customers' payments for services in the defendants' joint Skype-Microsoft telecommunications enterprise amount to wire fraud. Microsoft's role in subsequently blocking customers' access to the services - and deceiving customers about what really transpired – shaves cost from operating the joint telecommunication business and also - in the case of a few customers most determined to get what they paid for – brings it personal information from these customers that is lucrative for Microsoft's advertising and other businesses, but its actions are likewise fraudulent. Moreover, it should be noted that what happened to Plaintiff's Skype account and Microsoft account in January and June 2019 was not just two isolated events but akin to many similar incidents over the years that constitute a clear pattern. The defendants' use of "algorithm" further indicates that the fraudulent scheme has

been encoded in an automated system or process that is bound to repeat itself and is an ongoing criminal threat on a massive scale. Lastly, Plaintiff's interactions with the two defendants - the creation of each account and the making of payment - originated with each defendant's respective app or website, which proves each defendant's control and management of aspects of the fraudulent scheme, while the close corporate ties and operational coordination between the two defendants in technical support and customer service indicate joint participation in managing this racket.

17. Because of the series of fraud the defendants committed, Plaintiff not only lost money in direct payments to Skype but also suffered enormous financial losses due to lost time and lost opportunities and thus sues for monetary and statutory damages available under federal anti-racketeering statutes.

18. Plaintiff also sues to enjoin the defendants from requesting personal information that he did not surrender to Businesses at the start of service in any bargain to access, continue, renew the current level of services; to order Businesses to disclose how data of such personal information were collected, combined with Plaintiff's data that the defendants had previously collected, stored, handled, and distributed since January 2019; and to order the defendants to destroy said data.

19. The defendants have admitted that part of Microsoft Service Agreement was deliberately left vague and indefinite; that their own understanding and interpretation of what constitutes a customer's violation of the agreement evolves rapidly and at a monthly pace (more rapidly than the updates to the service agreement itself); and that the exact meaning and substance of the contractual provision about contractual breach by customers, which permits the defendants to unilaterally terminate service, is a secret that cannot be shared with customers – and is somehow not subject to judicial review. The defendants also knew at the time of executing the contract that Plaintiff was guaranteed to receive no consideration in return for his money. This deliberate vagueness and indefiniteness of substantial and vital provisions is unconscionable.

20. The unconscionability of the agreement also flows from the facts that Skype's services came pre-installed on Microsoft's operation system on Plaintiff's computer and that Plaintiff had little choice in looking for a international long-distance telecommunications provider that was not reliant on his cellular

service. Yet, the contractual terms were so lopsided and unreasonable that had Plaintiff – or any reasonable person - known that the defendants understood the contract he entered into at the time to mean that they needed to provide no service to him at all, he certainly would not have entered into the contract no matter how few other choices he had at the time.

21. The built-in vagueness in material provisions of the Microsoft Service Agreement and its substantive and procedural unconscionability render these provisions and the whole agreement void and unenforceable. Plaintiff thus sues to have his contracts with the two defendants declared void and null.

22. Alternatively, Plaintiff sues to have declared null and void any specific clauses and provisions that may be construed by the defendants to deny services to Plaintiff for using public or shared IPs. Such clauses are worded too vaguely to be enforceable, and they are unconscionable.

23. Plaintiff also sues Microsoft for intentional infliction of emotional distress under New York tort law. A serial identity theft victim who frequently saw his emails hacked into or his identity used by unauthorized parties to apply for jobs and credit, Plaintiff restarted an old habit of vigilantly watching over his accounts and emails in trying to spot any irregularities. Microsoft's agents and employees continued to affirm or otherwise equivocate throughout 2019 and 2020 about whether his accounts and emails were compromised, and their actions only served to deepen his anxieties about becoming an identity theft victim yet again, this time in still more intrusive way than before in that the thieves might have stolen a peep into all aspects of Plaintiff's daily life by situating themselves in his emails. This thought was a constant source of mental anguish for Plaintiff in the last two years, causing endless insomnia, migraines, and severe weight gains.

24. Microsoft's more recent statements that it was all a false warning should prompt one to question why the warning was worded the way it was. The language used in the false warning was bound to evoke any user's fear of identity theft and intrusion of privacy. The warning seems designed to have that very effect in hoaxing users into turning over their personal information to Microsoft in the misplaced hope that Microsoft would help the users to regain control. In other words, if the language caused users fear and distress, it is because it was meant to do so. Hence

the inevitable conclusion of Microsoft's malice and intent in inflicting such emotional distress on their users.

25. Therefore, Microsoft's willful and persistent lies and refusal to come clean to Plaintiff about what really transpired over the span of two years must be penalized because of its sheer malice in taking advantage of a consumer's vulnerability and past trauma of his struggles with lost access to the most important means of communications for and management of his personal and professional life and his struggles with big corporations in his attempts to reassert control over his own life.